IPv6 Business Conference

Organized by SWISS IPv6 COUNCIL

2016 June, 16

ERNW providing security.

Things to Consider When Deploying IPv6 in Enterprise Space

Enno Rey, erey@ernw.de

@enno_insinuator

Who Am I

- Old-school network security guy with some background in provider operations.
- Involved with LIR administration in some enterprise LIRs
  - Including the one with probably the coolest org handle: ORG-HACK1-RIPE.
- IPv6 since 1999 and regularly blogging about it at `www.insinuator.net/tag/ipv6`.

Agenda

- Address Strategy
- Routing
- Security Strategy

Case Study / Main Driver: Remote Access

Common IPv6 "initial use case" due to DS-Lite deployments (in cable networks)

- Questions to be clarified in advance
  - Addressing approach
  - Route propagation strategy
  - Some config elements of VPN devices

ERNW providing security.

How to Get Global IPv6 Addresses for $ORG

Approaches

- Use address space assigned from (one of) your provider(s)
  - Induces dependency, to be avoided.
- Apply for PI *assignment* from RIPE, through *sponsoring LIR*
  - At RIPE usually a /48 out of 2001:678::/29.
- (Become member &) Apply for PA allocation from RIPE
  - Usually a /29 out of 2a00::/12.

Once Decision Taken, another Question Comes Up

Out of region use

- “What can we reasonably expect on the Internet routing level when it comes to using this address space for subsidiaries/parts of our network outside of Europe and potentially announcing prefixes from local break-outs or regional hubs?”
- "(When) Does it make sense to apply for an IPv6 address space allocation at/from other Regional Internet Registries (RIRs)? All of them or 'the main ones'?“
- "If we opt for following the path of applying for allocations from several RIRs, what are the specifics/prerequisites/pitfalls of these procedures at the individual RIRs?
What about initial/recurring effort & costs?"

"Multiple Address Space"

Pros & Cons

See also:
http://www.ipv6conference.ch/wp-content/uploads/2015/06/B09-Rey_IPv6_Business_Conference_Address_Space_Approaches.pdf

- Pros
  - Consistent with initial mindset.
  - *Could* be helpful in the long-term
    - → Core of debate/speculation
- Cons
  - Creation of respective `route6` objects in different RIRs can be cumbersome/tricky.
    - In particular once outsourcing involved.
  - In the long-term potentially fragmented address space *within* global network.

"Cohesive Address Space" Approach

Pros & Cons

- Pros
  - Easier to handle wrt `route6` objects.
  - Unified address space in the long-term (as desired goal).
- Cons
  - Leads to *out-of-region* announcements
    - Good, bad, sth else?
  - - Needs renumbering if probs turn up later
    - DNS is your friend.
  - - Geo IP Location !?
    - Might be solvable, but considered significant issue by quite some global organizations.

Addressing Approach

Case Study / Decision Actually Taken

- For the moment go with "cohesive approach" and monitor situation/global (route) availability.
- Much easier handling with $SERVICE_PROVIDER expected.
- Allows to gain experience with
  - Out-of-region announcements
  - Provider capabilities
- We can always revert to use "multiple address space" approach.

A very Quick Word on IPv6 Address Plans

See also:
https://www.insinuator.net/2016/02/ipv6-address-planning-in-2016-observations/

- I've been involved in many address planning exercises myself and I had the opportunity to follow to what degree plans I've contributed to 12–24 months ago (some of them created in numerous iterations over several months) are actually implemented in operational reality
  - Want to guess?
- The main thing is to understand what makes sense in your organization
  - *Prescriptive* vs. *descriptive* strategy

Route Propagation/Handling

Potential Approaches (Sec Perspective)

See also:
https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-2-network-isolation-on-the-routing-layer/

- Selective announcements
  - Keep "strict filtering" in mind
- Null-routing/blackholing of (to-be) protected prefixes at network borders
  - E.g. prefix used for loopback addresses of network devices
  - This is what we see most often (planned).
- Reduced *hop limit* in specific segments

Routing Propagation Strategy

Variants Discussed in Case Study Env.

Overall long term strategy (in case study):
null-route specific prefixes which are supposed not to be reachable from untrusted networks.

- Implement long term strategy from the beginning
- For the moment go with *selective annoucements*, and monitor situation
  - As of today propagate only /48s

Start with *Selective Announcements* Strategy

Pros & Cons

See also:
https://www.troopers.de/media/filer_public/8a/6c/8a6c1e42-f486-46d7-8161-9cfef4101ecc/tr15_ipv6secsummit_langner_rey_schaetzle_slash48_considered_harmful_update.pdf

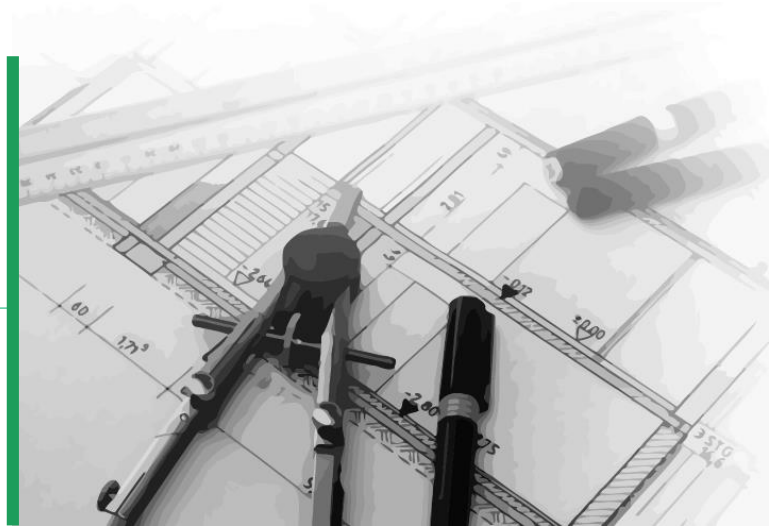
- Pro
  - one can gain experience with the approach and find out if "strict IPv6 prefix filtering" is (still) really a problem.
    One might note that currently ~46% of the IPv6 routes in the DFZ are /48s and the majority of those is without *covering aggregate*.
  - One doesn't get all the "usual noise" (network traffic from bots and the like) for a full /32 from the very beginning.
- Con
  - Potentially not aligned with long term strategy (which still might change though).

Routing Propagation Strategy

Case Study / Decision Actually Taken

- For the moment go with selective announcements (specific /48s only, see below).
  - Gain experience (not least as for $PROVIDER's maturity when it comes to route filtering & propagation).
  - Avoid noise.

Security Strategy

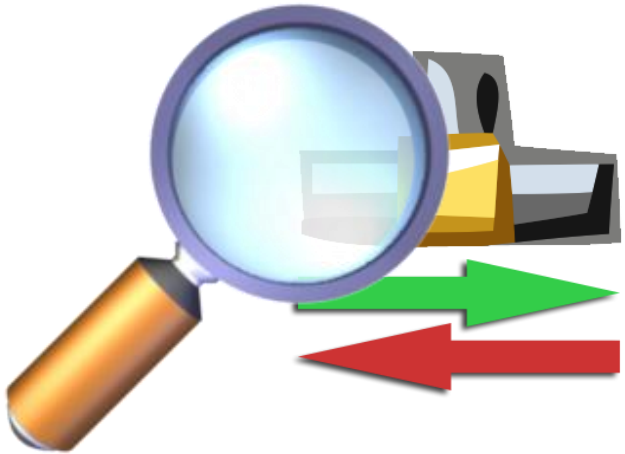


Security Strategy

- Includes
  - Traffic Filtering Approach, namely on border/perimeter devices
  - First Hop Security approach
  - Degree of static configuration vs. dynamic stuff (which is IPv6‘s DNA)

Infrastructure Controls

Traffic Filtering



- On network boundaries of the corp_nw and potentially intersection points within corporate network
  - Border gateways, business partners, WAN interconnection points
- IPv6-specific filtering rules to apply to prevent IPv6-specific threats
  - Do! Extension headers and/or fragments
  - Filtering of specific address ranges (multicast and un-assigned by IANA)
  - Apply specific rules wrt filtering ICMPv6.
  - Keep performance impact (in particular from logging) in mind!

Infrastructure Filtering

Discussion from a case study org

See also:

https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-3-traffic-filtering-in-ipv6-networks-i/

- Balance between
  - Visibility (of "bad stuff")
  - Speed
- ACL processing in itself shouldn't have too much performance impact on ASR 1K platforms.
  - Disable sending ICMPv6 Type1 might be required for hardware-only processing.
  - Protocol type-code access lists always on RP?
  - Optimized ACL Logging (OAL) might help. Supported for IPv6 and on specific platform?
- Logging desired/required? – For high speed Internet facing devices going with "drop only" might be preferable.

Filtering ICMPv6

Our recommendation for Internet border gateways

See also:
https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-4-traffic-filtering-in-ipv6-networks-ii/

```
permit icmp any any unreachable
permit icmp any any packet-too-big
permit icmp any any hop-limit
permit icmp any any parameter-problem
permit icmp any any echo-request
permit icmp any any echo-reply
permit icmp any any nd-ns
permit icmp any any nd-na
deny icmp any any log-input (?)
```

You may tweak this a bit, see: https://www.insinuator.net/2016/05/cve-2016-1409-ipv6-ndp-dos-vulnerability-in-cisco-software/

Infrastructure Controls

Filtering Extension Headers, Cisco


```
deny ipv6 any any routing
deny ipv6 any any hbh
[deny ipv6 any any fragments]
[deny ipv6 any any undetermined-transport]
deny ipv6 any any dest-option
deny ipv6 any any mobility
```

Infrastructure Controls

Filtering unallocated space

See also:
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

```
deny 0400::/6 any
deny 0800::/5 any
deny 1000::/4 any
deny 2d00::/8 any
deny 2e00::/7 any
deny 3000::/4 any
deny 4000::/3 any
deny 6000::/3 any
deny 8000::/3 any
deny a000::/3 any
deny c000::/3 any
deny e000::/4 any
deny f000::/5 any
deny f800::/6 any
deny fe00::/9 any
```

Infrastructure Controls

Filtering *Martians*


```
deny ipv6 host ::1 any log-input
deny ipv6 fc00::/7 any
deny ipv6 fec0::/10 any
deny ipv6 2001:db8::/32 any
deny ipv6 2001:2::/48 any
```

See also https://tools.ietf.org/rfc/rfc6890.txt

Infrastructure Controls

Alternative approach wrt address space filtering


```
deny ipv6 2001:db8::/32 any
permit ipv6 2000::/3 any
permit ipv6 fe80::/10 any
[permit ipv6 :: any]
deny ipv6 any any
```

VPN Use Case(s) / Setup

- Road warrior only or incl. S2S VPNs (business partners)?
  - For the latter see below.
- Keep in mind that, in context of a remote access solution, "IP connectivity" can actually mean two things:
  - Reach VPN gateways over IPv6
  - Be able to use IPv6 over/within tunnel

VPN Setup

Case Study / Decision Actually Taken

- Devices will be accessible over IPv6 but *no* IPv6 will be available within the tunnel.
  - No config of IPv6 address pools.
  - Else huge implications as for IPv6 addressing/routing in corp intranet.

How Do VPN Gateways Get Their Default Route?

Assuming they sit in $SOME_DMZ

- Perform full static configuration incl. address and default gateway
  - (Multi-) HSRP could come into play

  or

- Configure static address but learn default gateway from *Router Advertisements*
  - Clear PIO

ToDo

From case study organization

- Create `route6` objects for the involved /48 prefixes
  - Include $PROVIDER as `mnt-routes`?
- Announce routes via $PROVIDERS, leading to respective DCs/site(s)
  - Monitor propagation
  - Try going with /40 once affected by *strict filtering* (keep `route6` objects in mind!)
- Configure border gateways
  - Addresses on external/internal IFs
  - Proper (w/out PIO) *router advertisements* on inside IF
- Configure VPN gateways
  - Address(es) only, default route tb learned

Business Partner Connections with IPv6

Possible Approaches

Main differentiator is IPv6 source address of business partner connection.

- Inbound connection has source address from $ORGANIZATION's GUA prefix.
  - As a native address. and/or
  - Translated through NPTv6.
- Inbound connection has source address from $PARTNER's prefix.
  - Could potentially be GUA or ULA prefix.
- Inbound connection has source address from some other prefix.
  - E.g. from trusted 3rd party network (like, in automotive, the ENX/ANX networks) or some mutually agreed upon prefix.

Evaluation of Objectives

Case Study Organization

Objective	BP uses own prefixes, no translation, BP routes are redistributed	BP uses own prefixes, no translation, static routes at GWs (+ redist.)	BP uses own prefixes, those are translated via NPTv6	BP uses $ORG's prefixes for segments which establish connections	BP (& $ORG) use well-known/3rd party pref. (e.g. dedicated or ENX)
Manageability of routing	2 (low)	2 (low)	5 (very high)	5 (very high)	4 (high)
Feasibility to apply filtering/ACLs within DCN	2 (low)	2 (low)	3 (medium)	3 (medium)	4 (high)
Traceability ("Nachvollziehbarkeit")	5 (very high)	5 (very high)	2 (low)	3 (medium)	3 (medium)
Support of "isolation on routing layer"	1 (very low)	1 (very low)	3 (medium)	3 (medium)	3 (medium)
Stability of overall routing system	2 (low)	4 (high)	4 (high)	4 (high)	3 (medium)
Maintaining a cooperative relationship with BPs	4 (high)	4 (high)	3 (medium)	1 (very low)	3 (medium)
Overall operational feasibility	2 (low)	1 (very low)	3 (medium)	2 (low)	2 (low)
Sum of factors (equal weight assumed)	18	19	23	21	22

Summary

- In many organizations the advent of IPv6 might bring some paradigm changes.
- So before one “just enables IPv6 on something“ a number of decisions has to be taken.
  - Taking an easy (wrong) turn today may cost you dearly later.
- It helps to have a test lab ;-)

ERNW providing security.

There's never enough time...

THANK YOU...

...for yours!

@Enno_Insinuator

erey@ernw.de

Slides & further information:
https://www.troopers.de
https://www.insinuator.net
(..soon)

Questions?

Thanks to All Sponsors of the Event

Infoblox CONTROL YOUR NETWORK

f5

SWITCH

DIGICOMP

eb-Qual

itrain THE ESSENCE OF IT

Sunny Connection

BLUECAT

asecus securing your business

flowdays achieving more together

Image Credits

- Icons made by Freepik from www.flaticon.com are licensed by CC 3.0 BY.